DOCUMENT RESUME

ED 239 315 CS 504 418

AUTHOR	Shrader, Erwin
TITLE	Transborder Flow of Computerized Information: Controls and Restrictions.
INSTITUTION	Freedom of Information Center, Columbia, Mo.
REPORT NO	FOI-481
PUB DATE	Sep 83
NOTE	9p.
AVAILABLE FROM	Freedom of Information Center, Box 858, Columbia, Missouri 65205 ($1.00, quantity discounts available).
PUB TYPE	Information Analyses (070)
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	Business; Communication (Thought Transfer); Computers; Databases; Foreign Countries; Foreign Policy; Government Role; *Information Dissemination; Information Services; Information Sources; International Law; *International Relations; *Privacy; *Telecommunications
IDENTIFIERS	*Transborder Information Flow

ABSTRACT

Of major concern to United States position and policy in the telecommunications and information areas is "transborder data flow," the transferring of computer stored data between nations. Many European nations, including France, Austria, and West Germany, have enacted laws regulating the flow of information leaving the country where it would disrupt privacy. The bulk of automated data bases are located in the United States, which completely controls or manipulates most data exchanges between the U.S. and its partners. The U.S. is concerned that these protection laws, particularly those extended to "legal" persons such as corporations and institutions, will disrupt commerce and put American remote data processing at a disadvantage. Privacy protection for a country's citizens thus doubles as protection for its domestic computer industries. The Organization for Economic Cooperation and Development, representing 24 industrialized countries, has drafted guidelines for maximum standards of privacy protection to remove unjustified obstacles to transborder information flow, particularly of personal data. In the U.S., development of sound international communications policy has been disrupted by attention to domestic communications, although measures are pending in Congress. The U.S. delegation to a meeting of the General Agreement of Tariffs and Trade will propose making services subject to agreements now governing commodity trade in the hope of guarding against further international constraints on American information services. (HTH)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED239315

U.S. DEPARTMENT OF EDUCATION
NATIONAL INSTITUTE OF EDUCATION
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

X This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official NIE position or policy.

SCHOOL OF JOURNALISM, UNIVERSITY OF MISSOURI AT COLUMBIA

SEPTEMBER, 1983

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Freedom of Information Center

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

TRANSBORDER FLOW OF COMPUTERIZED INFORMATION: CONTROLS AND RESTRICTIONS

FREEDOM OF INFORMATION CENTER REPORT NO. 481

This report was written by Erwin Shrader, a master's degree candidate at the University of Missouri School of Journalism.

In November 1982, the U.S. Congress instructed the Commerce Department's National Telecommunications and Information Administration to study the nation's long-range goals in the areas of international telecommunications and information.

Five months later, the NTIA produced **An Outline for United States Policy**, a 288-page congressional report on international developments seen to be eroding American interests. It was alarming, (if not alarmist).

> It is important that remedial measures be initiated now. If we wait another ten years, before we counter these adverse trends — after seven more critical conferences and many more attacks on the free trade of goods, services, and ideas — it will be too late. The likely impact on U.S. defense capabilities, on employment and economic growth, and of freedom itself will be catastrophic.[1]

The NTIA study recounted at length the "adverse trends" in evidence internationally — politicization of the International Telecommunications Union, increased subsidization of computer and telecommunications industries by Japan and Western European nations, stepped up threats to worldwide press freedom — and layed out policy options and recommendations to help Washington shore up U.S. positions in the telecommunications and information arena.

Also of concern was the matter of "transborder data flow" — a relatively young communications and public policy phonomenon that has provoked the concern of U.S. government and business leaders.

THE ISSUE

Much, if not most, of the current discussion of "information" as a factor in the world-power equation pertains to Third World cultural and political concerns. Spokesmen for developing nations fear that Western media — as a dominant information force — misrepresent and often corrupt the relatively powerless inhabitants of those "lesser" nations. Thus, the calls for a new world order to rebalance the international information equation.

But another information equation is taking shape, and it's not a function of the traditional North-South, East-West divisions. Its components are not "biased" news reports and "corrupting" motion pictures, but rather raw data — the sort that can be sent almost instantaneously over great distances, to be sorted and stored by computers many, many miles away.

Attempts to define "transborder data flow" continue in the literature even as the technology that makes it possible advances.[2] Telephone, TELEX and the plodding mail have been used to transmit modest amounts of information across borders for decades, but the transborder flow of computer data is new and distinct.

The merging of telecommunications and computer technologies has allowed for the rapid transmission, storage and

Summary: The convergence of computer and telecommunications technology has made "transborder data flow" the subject of increased government attention. U.S. policymakers worry that Japanese and Western European data protection laws and trade barriers will put American businesses and information services at a disadvantage.

CS 504 418

computation of digitally encoded units of information. A remote data processing network, sucking up bits of information in one country and lickety-split making sense of them in another, goes beyond transatlantic TELEX or telephone conversation — or so the current debate over transborder data flow would suggest.

UNDERSTANDING THE PROBLEM

The debate, which came alive in the early 1970s, has quicksand qualities; the more you grab for solid ground and discrete points, the deeper you sink. One commentator called it, perhaps with some hyperbole, "the most complicated, convoluted and multifaceted issue of this century," involving as it does questions of national sovereignty and security, personal privacy and a society's economic health.[3]

But we may be certain of at least one point. At the root of the debate lies American dominance of the supply and use of information resources. The vast bulk of automated data bases are located in the United States, which completely controls or manipulates most data exchanges between the Unites States and its partners.[4] The oft-noted use of a Cleveland-based computer by the fire department of Malmo, Sweden indicates the nature, if not the level of dependence.[5]

The United States' historical dominance of computer design and manufacture cannot be overlooked. It hasn't been by the French government, which in its 1977 Nora-Minc study, warned of foreign computer firms, primarily IBM, becoming instruments of foreign domination. To counter American control of the domestic computer market, the French government, according to the report, had to begin viewing mastery of computer technology as being as important as nuclear mastery. The first of its kind, the Nora-Minc study made explicit the importance of indigenous control of computerized information to the economic and political vitality of a nation.[6]

Through technological advances, data can be processed, stored and transmitted faster and in greater amounts than ever before. In short, it's a powerful tool, easily exploited by its users, be they governmental or commercial.

With its data stored abroad, a nation becomes dependent on the servicing country's being politically and economically stable. A data "black-out," caused by accidental or intentional interruption of national and international data communications, could leave a number of countries and organizations extremely vulnerable.[7] Thus, in much the same way an aspiring national power develops and maintains indigenous steelmaking capabilities, a government must nurture an information infrastructure that includes data bases.

Economic self-determination also can be threatened by transborder data flow (though it can likewise be enhanced). More and more financial decision-making is done extraterritorially by multinationals such as IBM using increasingly sophisticated communications technology. With this kind of technology available, a nation could become economically handicapped if its data processing industry fails to mature. Thus, the dictum is simple, if circular: Design and build computers at home, keep information at home and use information to keep jobs at home, notably jobs in burgeoning information-related services and manufacturing.

No less important is the need for nations to insure the rights of its citizens against alien usurpers. Transborder data flow, various governments have come to realize, confounds their ability to do so, principally as regards personal privacy. While within legal boundaries, information deemed personal, and therefore restricted, is protected by national law. If it allows that information to come to rest in a data base in a country with weaker or dissimilar regulations, a nation forfeits the authority to protect the privacy of its own.

How to frame the myriad concerns of nations facing the realities of transborder data flow? One observer suggests that it's brought about a new complexity in international relations.

> These issues (relating to data flow) can usefully be conceptualized as nothing more than modern expressions of age-old rivalries in industrial, trade and political areas. Yet those modern expressions of legitimate national concern are somewhat different from, and in many ways more subtle than, the traditional issues. "Information" as a rubric is both pervasive and difficult to define — omnipresent, but quiet and unobtrusive in ordinary political and commercial contexts. No fully adequate tradition for dealing with these matters exists, and yet there is a growing awareness of their importance.[8]

That awareness, however, has amounted to "nothing more than modern expressions of age-old rivalries," according to American business leaders.[9] As **An Outline for United States Policy** would have it, leaders believe, barriers to transborder data flow, whether in the form of restrictions on data, on channels of telecommunication, or on sale of computer and communication technology, have materialized in Western Europe, in Japan and even in certain developing countries. According to a former NTIA policy maker, the restrictions are protectionist and could lead to the exploitation of "the general shift toward an information-based service economy."[10]

EUROPEAN CONTROLS

Data Protection Laws

Direct regulation of transborder data flow began with the non-economic concern in Europe that the computerization of information posed a real, if not fully realized, threat to individuals. Anxiety about data processing stems from the individual's loss of control over data concerning his rights and interests, such as salary, health and credit.[11] To amend this situation, European governments throughout the 1970s enacted a variety of national laws guaranteeing citizen access to, and the security of, electronically stored personal data. The European laws incorporate many of the same fair information practices found in the United States' Privacy Act, Fair Credit Reporting Act and Freedom of Information Act (although, as we shall see, profound differences exist).[12]

Focusing as they do on automated data, the majority of European privacy protection laws contain articles regulating transborder data flow as an adjunct to the more general regulation of the storage and use of data. As noted above,

European legislators realized the futility of instituting fair information practices in their countries when the same personal data could be electronically transmitted to, and stored in, a country without similar protections. A look at transborder data flow provisions in the data laws of Sweden, France and West Germany is instructive.

Sweden — The premier and prototypic data protection law is the Swedish Data Act of 1973.[13] Under this national law, the formation of a data bank that will contain personal information is subject to prior approval by the Data Inspection Board, a government agency headed by an 11-member directorate. All data transmissions are subject to general regulations enforced by the Data Board. In addition, those crossing national boundaries must be granted specific board approval.

As a general rule, all companies operating in Sweden are required to process information on Swedish citizens in Sweden itself, although the Data Board may grant exemptions. Such exemptions are hardly "pro forma," according to one author, who cites the Board's refusal, in 1975, to allow Siemens to send data on Swedish employees for inclusion in a central personnel file at the multinational's computer center in Munich.[14]

France — The French statute requires private entities intending to store and transmit personal information in France to notify the governmental National Data Processing and Liberties Commission.[15] The notification must indicate whether data processing is intended for the dispatch of personal data between France and another country. The French statute does not require prior approval for storage and transmission. It does, however, give the Data Commission the discretionary authority to make particular transborder data flow activities subject to prior approval after the initial notification process.

West Germany — The German Data Protection Act, instituted in 1977, does not deal explicitly with transborder data flow, but certain provisions are clearly applicable.[16] Notably, data processors are prohibited from disseminating or storing data if the privacy rights of the data subject stand to be violated. On this basis, the absence of a suitable data protection law or provision at the data's destination is grounds for disapproval. Advance approval of transborder data flow links, however, is not required under the act.

AMERICAN CONCERNS

To date, ten European nations have proposed or enacted data protection laws, with those of Austria and Denmark being the most restrictive. Despite their diversity they share characteristics alien, if not unsettling, to certain American commercial and governmental interests. These concerns were voiced in testimony before a U.S. House of Representatives subcommittee in March and April of 1980 and were summarized in the committee's report, **International Information Flow: Forging a New Framework**, issued later that year.

The report's authors alert readers to important differences between United States' privacy statutes and the data protection laws of Europe. The European laws, they explain, are all national statutes establishing regulatory boards or commissions and concentrating on computerized data and its transmission.[17] These "omnibus" efforts, in addition, apply to both public and private record-keeping, while "providing little protection from access by government to information about citizens."[18]

Indulging in jurisprudence, the report points to the reliance of American law on the individual seeking to redress actual injury as, perhaps, the reason for the fundamental differences in privacy legislation.

> (A)n essential difference exists between the focus of legal protection in American and European law. The administrative schemes of the European statutes go to protecting the information maintained in data banks. The statutes seek to build a wall around a particular classification of information. U.S. law seeks to protect the person, the individual who may be injured by misuse of information about him. . . .It is injury, not release "per se," that is punishable.[19]

But American concern with Europe's data protection laws, as reflected in the congressional document, is not simply quirkish intolerance of a different legal tradition. Data protection on the other side of the Atlantic — especially that extended to "legal" persons, i.e., corporations and institutions — threatens to disrupt commerce, the 1980 report diplomatically suggests.

> Although the sincerity of the European concern for privacy cannot be doubted, their particular approaches to protecting privacy and their lack of distinction between individual human beings and legal persons such as corporations threatens serious economic repercussions for all national and real conflicts with U.S. law and policy.[20]

Slowing or in some cases stanching the transborder flow of computerized information, and European privacy legislation puts American remote data processing at a disadvantage, whether conducted by firms selling that very service or by U.S.-based multinationals going about their business.[21] Privacy protection for a country's citizens thus doubles as protection for domestic computer industries. Again, the authors of **Data Flow Report** voice American concern and issue a warning.

> If unnecessarily burdensome or employed as tools to achieve other ends, such as the protection of economic interest, the best international safeguards for individual rights will be eroded by cynicism about their true intent.[22]

And so the line of demarcation between privacy and commercial protection blurs. Information "offenses," like that heralded by the Nora-Minc report, confirm in the minds of American policy-makers what data laws only suggested.[23] A trade war brews, to include, as we shall examine next, stepped-up government regulation of the international communication channels.

FURTHER RESTRICTIONS

Data protection laws affect transborder data flows by monitoring data content and sifting out restricted personal information. Less discriminatory, yet equally significant in altering the patterns and volumes of data flow, is government regulation of the channels of computer telecommunication (principally, satellite and underwater cable). Of ongoing and growing concern to American telecommunications principals are the so-called non-tariff trade barriers they see blunting American commercial efforts in the area of worldwide data services. Given the prominence of American data services worldwide and the heavy overseas investment of U.S. multinationals, the United States, they argue, has the most to lose economically if regulations tighten.[24]

To understand European and Japanese efforts to get bigger pieces of the international data flow action, one must understand the significant powers of the typical Ministry of Posts, Telephones and Telegraph, or PTT. Found in every Western European nation (Japan operates through a designated carrier), PTTs constitute a government monopoly over telecommunications equipment and services.

Because of the absence in Europe of basic private sector involvement — involvement characterizing both domestic and international communications systems in the United States — the PTT acts not only as the regulator, but also as the regulated.[24] As such, a PTT is in a position to formulate and enforce telecommunications policies that unabashedly promote its own telecommunications services and policies.[25] Of late, some such policies have been used to alter or impede transborder data flow either through increased cost or explicit restriction. Two examples will suffice, one involving Japanese government action on behalf of its international record carrier, Kokusai Denshin Denwa Co. (KDD), and the other the West German Budnespost.

Central to both affairs is the preferred use of the so-called private leased line by certain commercial customers — most often banks, multinational businesses and data processing services. Made available by PTTs and U.S. common carriers at flat monthly rates, private circuits have proved a bargain for heavy users as compared to purchase of usage-sensitive services, such as TELEX (which charges by length of time). Moreover, exclusive access to a circuit lets a user attach computer equipment to suit particular needs (including resale of the use of the circuit) and to increase the amount and accuracy of the data transmitted.

Thus, as advances in computer-telecommunications technology have increased the efficiency of these lines, the relative cost to the individual user has decreased. This has encouraged greater use of leased circuits — all without the intervention of, and without any significant increase in revenues for, the PTTs and participating carriers, who generally lacked the technical sophistication to discern the amount of data transiting the lines.[27] As the affair involving Japan's KDD and two American firms will show, in the future, private lines will be made available at considerably greater expense and with less flexibility — much to the disadvantage of American multinationals and international information services.

In 1978, two American computer companies and international information companies, Control Data Corp. and Tymshare, Inc., decided to offer a broad range of data processing services to clients in Japan, using computer mainframes located in the United States. They entered into negotiations with KDD.

About four years later, Control Data and Tymshare were let into the Japanese market. Both have obtained leased lines from KDD, but the lease agreements until recently contained restrictions that severely impeded the companies' ability to provide services and compete effectively in Japan.[28] Most significantly, both were prohibited from connecting the leased line to more than one computer center in the United States. Consequently, although Control Data, for example, has five different data processing locations in the United States, each performing distinct types of operations, it could offer Japanese customers only the services of the one computer hookup. Moreover, the lease agreement was accompanied by the demand that once KDD has instituted its proposed usage-sensitive network, the two American firms would be expected to make use of it.

The effect of the switch to the new service, said a Tymshare executive during congressional testimony, would be to increase the price of the company's computing services in Japan by ten times, rendering Tymshare incapable of competing effectively in the Japanese domestic computer service market.[29]

The more recent example of a nontariff trade barrier affecting the pattern of transborder data flow, to the disadvantage of American interests, involved the West German PTT, the Bundespost. A Bundespost regulation, put into effect in 1982, required all foreign data processors to transfer their transatlantic and other international traffic to more expensive usage-sensitive services offered by the Bundespost — but with one notable exemption. Private leased lines, it was stated, would be made available to foreign data services on the condition that the computer company maintain significant data computer processing facilities within Germany. The exemption could defeat many of the economic and technical advantages of operating a worldwide data processing network, according to one observer.

> In both purpose and effect, the Bundespost regulations are nontariff barriers to trade. The regulations not only protect West Germany's data processing services industry (and the jobs it provides), but they also assure that the Bundespost will derive higher revenues.[30]

These two cases by no means exhaust examples cited by American policymakers of PTT telecommunications regulations impeding entry into international data-service markets, an associated effect of which is the increase in operational costs for American businesses operating overseas. The NTIA's report, for one, includes in its list of "anticompetitive measures" the levying of special taxes on communications circuits used in specific ways and the "imposition of inconsistent or narrowly interpreted technical standards" for both providers and users of telecommunication and data processes. There are, in addition, a host of Japanese and European trade policies designed primarily to bolster indigenous information industries.[31]

Thus the circle widens. American attention turns from the

relatively benign data protection law to the more disturbing nontariff trade barrier, posing inconvenience and competitive disadvantage for American businesses that depend on the "free" flow of automated data.

But one additional threat haunts such businesses — the systematic valuation and taxation of data flow, such as that proposed in 1980 by the chairman of the French Commission of Transborder Data Flows.[32] Fearing that national interests would be subordinated to the interests of multinational businesses, the chairman pointed to the "value" of computerized data crossing national boundaries. That traffic, he argued, should be subject to the same tariff principles that apply to physical goods that have value and cross borders. Furthering his proposition, the chairman, in a report on legal and economic aspects of transborder data flow, outlined a data classification scheme that among other things, defined information in terms of its contribution to the process of creating a final product.[33]

The U.S. government's response to comprehensive valuation of automated data — as presented in the NTIA report — is less than enthusiastic. While granting that under certain circumstances information "can be packaged and sold just as any 'commodity,' " with its market value established by seller and buyer, the report suggests that the bulk of commercial information serves some "intermediate function" in the production process.[34va2] Such information, the authors maintain, certainly contributes to the ultimate value of a final product, but itself has no "market value" to serve as an objective basis for taxation. Opposing any move towards data valuation and taxation **Outline for United States Policy** recommends:

> The U.S. position on this matter, consistent with the long-range goals of promoting the role of telecommunications and information technology as a contributor to the efficient utilization of resources, would be to strongly oppose any actions that would interfere with the ability of producers and users to make optimum use of information as a productive resource.[35]

Equally compelling a reason for opposing classification, the authors add, is the obvious need for surveillance of data content in the process of evaluation. "This could lead to dangerous abuses of personal and proprietary information," the report reads — bringing us, ironically, full circle, back to privacy.[36]

WHAT'S IN STORE

> Conflicts over the integration of telematics into the world society give every promise of growing broader, deeper and sharper. Against a backdrop of protectionism, high unemployment rates, stagflation, and a new fragility in postwar political allegiances, unexpected tensions and antagonisms may be expected to emerge from the computerization of society itself.[37]

Amidst the gloom of the preceding prognosis, it might be useful to examine international efforts to contend with the matter of personal data and transborder flow. The primary forum for a "negotiated peace" has been the Organization for Economic Cooperation and Development, an independent body comprising representatives from 24 industrialized countries. In 1978, the OECD, which had been active in the area of data protection since early in the decade, decided to address the problems of diverging national legislation and established a new intergovernmental Expert Group on Transborder Data Barriers and the Protection of Privacy. The following year the group presented draft guidelines governing transborder data flow and the protection of personal data and privacy, in order "to facilitate the harmonization of national legislation."[38va2] The guidelines, which are nonbinding, were adopted by the OECD in September 1980 and signed by the United States.

They outline maximum standards of privacy protection drawn from principles identified in the U.S. Privacy Act of 1974, including:

- limitations on the collection of personal data;
- requirements that what is obtained be relevant, accurate, complete, and up-to-date;
- specification of the purposes for which the data will be used;
- limitations on disclosure without the subject's consent or by authority of law;
- safeguards against unauthorized access;
- openness about developments, practices and policies with respect to personal data; and
- the right of subjects to see information about them and to challenge, correct or amend it.

More generally, the guidelines urge member countries to take the recommendations into account in domestic legislation, to remove unjustified obstacles to transborder flows of personal data, to cooperate in implementing the guidelines, and to agree as soon as possible on a "specific mechanism of consultation and cooperation."[39]

For its part, the United States "instituted a successful program to inform private sector firms about the guidelines and to seek their support through voluntary adoption of policies that adhere to the principles set down."[40va2] Approximately 180 major corporations and trade associations, according to the NTIA, publicly endorsed the guidelines. Clearly it is the voluntary nature of the agreement, a document with no formal enforceability, that is attractive to American policymakers.[41] Moreover, controversial concepts, i.e., the extension of data protection to legal persons, are either absent from the guidelines or worded in a way allowing for wide interpretation. "Their non-binding character," says the House's 1980 report of the Guidelines, "preserves the flexibility which is vital in adapting broad international policies to different legal and governmental systems."[42]

The United States' relatively enthusiastic reception of the guidelines (after all, they were heavily influenced by the American delegation) contrasts sharply with that given another international data protection document, namely, the Council of Europe's "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." The Convention, which was adopted in October 1980

by the 21-member body, is potentially more restrictive than the OECD Guidelines and, furthermore, requires signatories to pass implementing legislation.[43] Such legislation would entail enactment of an all-encompassing statute covering computerized personal data held privately or by the government, as well as the requirement that data bases be registered with a central authority.

Under the convention, parties may modify the treaty's coverage to include legal persons and manually processed files. Although the United States sends observers to Council of Europe meetings, the government has kept its distance from the convention, which most likely will be ratified and in effect in member states by the end of 1983.[44]

"The U.S. position," states the congressional data flow report, "reflects the belief that transborder data flow problems and resulting policy positions are at too early a stage of development to warrant binding agreements."[45] The authors of the NTIA report, commenting on the Council's Convention, are not as disposed to explication: "The United States, does not approach privacy protection this way," the report states.[46]

Much of the literature on transborder data flow deals with the formulation of international privacy legislation, of which the OECD Guidelines and the Council of Europe Convention are the most significant practical models. One author warrants that such models finding their way into international law may prove to be "no more than scattered intermittent interruptions to the onward thrust of technological advance," especially if a growing network of digitallized transmissions stew together increasing amounts and kinds of information. (How, for example, would a news reporter's notebook, transmitted digitally, be treated by a nation's data commission?)

For now, the OECD Guidelines are what Japan and the industrialized West have to show for their legislative efforts. Few commentators suggest the guidelines will impose strict order on transborder data flow. Rather, their usefulness lies in "memorializing the basic, agreed upon principles of privacy protection" and in providing a framework for coordinating the domestic efforts of participating countries.

However, as we have seen, the scope of American concern over the evolving matter of transborder data flow extends beyond privacy protection. Technological advance and economic efficiency in the transmission of personal and nonpersonal computerized data, it is said, are endangered by the increasing politicization by other nations of telecommunications and information. In defense of its global interests, the United States' course is clear, according to **An Outline for United States Policy**:

> Technology develops most felicitously in an environment wherein it is thought to be largely value-free . . . . The first objective ofU.S. policy in the telematics field therefore must be to deflect discussion as far as possible into technical rather than substantive political circles.

INACTION AND REORGANIZATION

But what is the United States' international telecommunications and information policy? And who is making it? These are questions subsuming more particular concerns about transborder data flow, while confounding political observers in Washington.

With administration and congressional attention focused on domestic communications — what with the divestiture of AT&T — international policy at best has been neglected. At worst it has become disputed territory, involving primarily the Commerce Department, the State Department and the United States Trade Representative.

"The inaction," says the counsel to a House of Representatives government operations subcommittee, "is largely a result of turf battles and ignorance."It is a situation, he says, which is not helped by the complexity of international telecommunications.

Within just the past few months a position was created within the State Department for the "coordination and formulation of communications and information policy." The action, as viewed by some, has succeeded in offending the Commerce Department's NTIA and has assured continued fractured policymaking — this at a time when the NTIA reportedly has been gutted by budget cuts and poor administration.

One of the NTIA's very own proposals, in its March 1983 report, is aimed at remedying disjointed decisionmaking on matters such as transborder data flow. **An Outline for United States Policy** recommends a revamping of telecommunications and information policymaking in the executive branch. The recommendation, in good part, has been incorporated in a bill now with the Senate Subcommitte on Communications.

The International Telecommunications Act of 1983, sponsored by Sen. Barry Goldwater, would create an office for telecommunications and information within the executive branch. It would also establish a task force comprising relevant departments and agencies to be the principal coordinating body for the development of U.S. telecommunications and information policy. In addition to policy coordination, further deregulation of international telecommunications service and "reliance whenever possible on marketplace competition" are objectives of S. 999.

A similar measure entailing reorganization (H.R. 2527) has been introduced in the House of Representatives by Rep. Glenn English. But H.R. 2527 has languished, as did comparable bills initiated by English in the 96th and 97th Congresses.

Information policymaking is dead in the water, according to a member of English's staff, in part because it's just plain difficult to figure out what needs to be done substantively. "It's more a matter of creating a power center and seeing what happens," the staff member says. "We need an office that will say 'Thank you for your views, now here is what is going to happen.' "

For now, specifically in the area of transborder data flow, the Reagan administration continues to monitor the progress of the Council of Europe's Convention. In addition, the

United States has representatives participating in OECD working groups now studying legal and economic aspects of transborder data flow.

On a broader front, the U.S. delegation to a ministerial meeting on the General Agreement of Tariffs and Trade in November plans to present a position paper on making services subject to agreements now governing commodity trade. Such agreements, it is hoped, would guard against further international constraints on American information services.

When it comes to national security, the Reagan administration, of course, is not above restricting the American information sector — most notably manufacturers and exporters. The International Traffic in Arms Regulations and Export Administration Regulations have been mobilized as concern grows that the Soviet Union and its allies have benefitted unduly from technology transfers in, among other areas, those of computer and telecommunications.

But overall it is quite clear that fewer not more restrictions on information and related technologies serve American interests. What remains unclear, however, is how American concern over data protection laws and nontariff barriers will take on definite shape through government reorganization and policy.

FOOTNOTES

1. U.S. Congress, Senate, **Long-range Goals in International Teleccommunications and Information: An Outline for United States Policy**, 98th Congress 1st Session, 11 March 1983, p. xii.
2. Eric Novotny, "Transborder Data Flows and International Law: A Framework for Policy-oriented Inquiry," **Stanford Journal of International Law**, Summer 1980, p. 141.
3. John Eger, "Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers?" **Law and Policy in International Business**, 1978, p. 1055.
4. William Fishman, "Introduction to Transborder Data Flows," **Stanford Journal of International Law**, Summer 1980, P. 1.
5. A data base in a General Electric computer contains a comprehensive list of hazardous materials in Malmo. When a fire alarm is signaled, the computer communicates to the fire department what hazardous materials are at the particular site.
6. Fishman, p. 9.
7. Joseph Schickich, Jr., "Transborder Data Flows," Law and Computer Technology, 3rd Quarter 1978, p. 62.
8. Ibid.
9. Fishman, p. 14.
10. Arthur Bushkin, "The Threat to International Data Flows," **Business Week**, 3 Aug. 1981, p. 10.
11. A.C. Evans, "European Data Protection Law," **American Journal of Comparative Law**, Fall 1981, p. 1.
12. Novotny, p. 169.
13. See generally, M.D. Kirby, "Transboder Data Flows and the 'Basic Rules' od Data Privacy," **Stanford Journal of International Law**, Summer 1980, p. 27. Evans, p. 574.
14. Mark Feldman and David Garcia, "National Regulation of Transborder Data Flows," **North Carolina Journal of International Law and COmmercial Regulation**, Winter 1982, p. 1.
15. See generally, Feldman, p. 15. Kirby, p. 37.
16. See generally, Kirby, p. 38. Schichkich, p. 68.
17. U.S. Congress, House of Representatives, **International Information Flow: Forging a New Framework**, 96th Congress 2nd Session, 1980, p. 38.
18. Ibid.
19. Ibid., p. 40.
20. Ibid, p. 3.
21. Bushkin, p. 10.
22. U.S. Congress, House of Representatives, p. 5.
23. Eger, **Denver Post**, p. 19.
24. U.S. Congress, House of Representatives, p. 27.
25. Joseph Markoski, "Telecommunications Regulations as Barriers to the Transborder Flow of Information," **Cornell International Law Journal**, Summer 1981, p. 141.
26. Ibid.
27. Ibid., p. 298.
28. Feldman, p. 4.
29. Statement of Warren E. Burton, vice president, in Feldman, p. 4.
30. Markoski, p. 287.
31. U.S. Congress, Senate, p. 6.
32. Ibid., p. 193.
33. Eger, **Cornell International Law Journal**, p. 221.
34. U.S. Congress, Senate Committee on Commerce, Science, and Transportation, p. 194.
35. Ibid., p. 195.
36. Ibid.
37. Dan Schiller, **Telematics and Government** (Norwood, N.J.: Ablex Publishing, 1982), p. 187.
38. "Draft Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," OECD Doc. DSTI/ICCP/79.40 (December 1979), reprinted in **Computer Networks**, 1981.
39. Ibid.
40. U.S. Congress, Senate, p. 192.
41. Ibid., p. 192.
42. U.S. Congress, House of Representatives, p. 20.
43. Eger, **Cornell International Law Journal**, P. 217.
44. U.S. Congress, Senate, p. 246.
45. U.S. Congress, House of Representatives, p. 20.
46. U.S. Congress, Senate, p. 191.
47. Kirby, p. 27.
48. Fishman, p. 18.
49. Schiller, p. 146.

Additional copies of this report, and other Freedom of Information Center reports, may be obtained by writing the Center at Box 858, Columbia, Missouri 65205. There is a $1 charge for each single copy, 90 cents each for 25 or more copies, $60 per 100 copies, and $50 per 100 on orders of 300 or more copies.